

Amendments to the claims

This listing of claims replaces all prior versions and listings of claims in this application.

What is claimed is:

1. (Currently amended) A security architecture for a computer platform comprising at least one data processor and at least one memory means said architecture comprising:

an applications layer ~~(200)~~ for containing a plurality of user security applications;

a layered services layer ~~(201)~~ for containing a plurality of security services protocols;

~~a language interface adapter, and tools for policy and model authoring or the like;~~

a common security services manager (CSSM) layer ~~(202)~~ underlying the layered services layer comprising a plurality of security services management means ~~(203-208)~~, a set of integrity services, ~~a policy interpreter,~~ a manager of security contexts, and a plurality of interfaces ~~(209-214)~~ for interfacing with add-in security modules ~~(216-221)~~; and

an add-in security modules layer ~~(215)~~ capable of accepting underlying the common security services manager layer, configured to accept a plurality of add-in security modules ~~(216-221)~~ implementing a set of standard security services;

~~characterized in that said architecture comprises;~~

a generic trust policy library ~~(217)~~ within the add-in security modules layer and supporting a set of standard trust policy Application Programming Interfaces (APIs) ~~and some functions dealing with trust policy description files;~~

a trust policy description file ~~(223)~~ containing a set of domain-specific trust policies written in a policy description language common to said architecture; and

a policy interpreter ~~(224)~~, said policy interpreter operating to interpret a set of policies contained in said policy description file.

2. (Currently amended) The architecture as claimed in claim 1, ~~characterized in that wherein~~ at least one of said plurality of said management means ~~(203-208)~~ is provided with a corresponding respective policy description file determining the policies with which said at least one management means operates.

3. (Currently amended) The architecture as claimed in claim 1, ~~characterized by further~~ comprising a set of policy and model authoring tools ~~(400)~~, allowing a user to create said policy description file implementing a set of user specified domain-specific policies for controlling said computer platform.

4. (Currently amended) The architecture as claimed in claim 1, ~~characterized in that wherein~~ said policy description language comprises a known PROLOG language.

5. (Currently amended) The architecture as claimed in claim 1, ~~characterized in that wherein~~ said policy interpreter comprises a PROLOG inference engine.

6. (Currently amended) The architecture as claimed in claim 1, ~~characterized in that wherein~~ said common security services manager layer ~~(502)~~ is provided with its own policy description file ~~(520)~~ for implementing policies in that layer.

7. (Currently amended) The architecture as claimed in claim 1, ~~characterized in that wherein~~ said applications layer ~~(500)~~ is provided with an applications layer policy description file ~~(540)~~ for determining policies to be implemented in said applications layer.

8. (Currently amended) The architecture as claimed in claim 1, ~~characterized in that~~wherein said layered services layer ~~(501)~~ is provided with a layered services layer policy description file ~~(506)~~ for determining policies followed by said layered services layer.

9. (Currently amended) The architecture as claimed in claim 1, ~~characterized in that~~wherein at least one of said plurality of add-in security modules ~~(216, 218-221)~~ is provided with a corresponding respective policy description file determining the policies with which at least one add-in security module operates.